

## § 806b.5

- (5) Review system notices.
- (6) Investigate complaints.
- (7) Staff denial recommendations (at MAJCOMs and FOAs only).
- (g) System Managers:
  - (1) Decide the need for, and content of systems.
  - (2) Manage and safeguard the system.
  - (3) Train personnel on Privacy Act requirements.
  - (4) Protect records from unauthorized disclosure, alteration, or destruction.
  - (5) Prepare system notices and reports.
  - (6) Answer Privacy Act requests.
  - (7) Keep records of disclosures.
  - (8) Evaluate the systems annually.
- (h) Privacy Act Monitors (PAM):
  - (1) Are the focal point in their functional area for general Privacy Act questions and correspondence.
  - (2) Maintain a list of all systems of records and system managers in their area.
  - (3) Act as liaison with the Privacy Act Officer.
  - (4) Maintain statistics for the annual Privacy Act report.

## Subpart B—Obtaining Law Enforcement Records and Promises of Confidentiality

### § 806b.5 Obtaining law enforcement records.

The Commander AFOSI; the Chief, Air Force Security Police Agency (AFSPA); MAJCOM, FOA, and base chiefs of security police; AFOSI detachment commanders; and designees of those offices may ask another agency for records for law enforcement under 5 U.S.C. 552a(b)(7). The requesting office must indicate in writing the specific part of the record desired and identify the law enforcement activity asking for the record.

### § 806b.6 Promising confidentiality.

Record promises of confidentiality to exempt from disclosure any 'confidential' information under subsections (k)(2), (k)(5), or (k)(7) of the Privacy Act.

## 32 CFR Ch. VII (7–1–98 Edition)

## Subpart C—Collecting Personal Information

### § 806b.7 How to collect personal information.

Collect personal information directly from the subject of the record when possible. You may ask third parties when:

- (a) You must verify information.
- (b) You want opinions or evaluations.
- (c) You can't contact the subject.
- (d) The subject asks you.

### § 806b.8 When to give Privacy Act statements (PAS).

- (a) Give a PAS orally or in writing:
  - (1) To anyone from whom you are collecting personal information that will be put in a system of records.
  - (2) Whenever you ask someone for his or her Social Security Number (SSN).

NOTE: Do this regardless of how you collect or record the answers. You may display a sign in areas where people routinely furnish this kind of information. Give a copy of the PAS if asked. Do not ask the person to sign the PAS.

- (3) A PAS must include four items:
  - (i) Authority: The legal authority, that is, the United States Code or Executive Order authorizing the program the system supports.
  - (ii) Purpose: The reason you are collecting the information.
  - (iii) Routine Uses: A list of where and why the information will be disclosed outside DoD.
  - (iv) Disclosure: Voluntary or Mandatory. (Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information.) Include any consequences of nondisclosure in non-threatening language.

### § 806b.9 Requesting the social security number (SSN).

- (a) Do not deny people a legal right, benefit, or privilege for refusing to give their SSNs unless the law requires disclosure, or a law or regulation adopted before January 1, 1975, required the SSN and the Air Force uses it to verify a person's identity in a system of records established before that date.

When you ask for an SSN to create a record, tell the individual:

(1) The statute, regulation, or rule authorizing you to ask for the SSN.

(2) The uses that will be made of the SSN.

(3) If he or she is legally obligated to provide the SSN.

(b) The Air Force requests an individual's SSN and provides the individual information required by law when anyone enters military service or becomes an Air Force civilian employee. The Air Force uses the SSN as a service or employment number to reference the individual's official records. When you ask someone for an SSN as identification (ID) to retrieve an existing record, you do not have to restate this information.

(c) Executive Order 9397, November 22, 1943, authorizes using the SSN as a personal identifier. This order is not adequate authority to collect an SSN to create a record. When law does not require disclosing the SSN or when the system of records was created after January 1, 1975, you may ask for the SSN, but the individual does not have to disclose it. If the individual refuses to respond, use alternative means of identifying records.

(d) SSNs are personal and unique to each individual. Protect them as FOR OFFICIAL USE ONLY (FOUO). Do not disclose them to anyone without an official need to know.

### Subpart D—Giving Access to Privacy Act Records

#### § 806b.10 Making a request for access.

Persons or their designated representatives may ask for a copy of their records in a system of records. Requesters need not state why they want access to their records. Verify the identity of the requester to avoid unauthorized disclosures. How you verify identity will depend on the sensitivity of the requested records. Persons without access to notary services may use an unsworn declaration in the following format: 'I declare under penalty of perjury (if outside the United States, add 'under the laws of the United States of America') that the foregoing is true and correct. Executed on (date). (Signature).'

#### § 806b.11 Processing a request for access.

Consider a request from an individual for his or her own records in a system of records under both the Freedom of Information Act (FOIA) and the Privacy Act regardless of the Act cited. The requester need not cite any Act. Process the request under whichever Act gives the most information. When necessary, tell the requester under which Act you processed the request and why.

(a) Requesters should describe the records they want. They do not have to name a system of records number, but they should at least name a type of record or functional area. For requests that ask for 'all records about me,' ask for more information and tell the person how to review the Air Force systems of records published in the FEDERAL REGISTER or in AFDIR 37-144<sup>1</sup>, 'Privacy Act Systems of Record' (formerly AFR 4-36).

(b) Requesters should not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making Privacy Act requests. Privacy Act Officers and system managers process such requests but tell requesters that using government resources to make Privacy Act requests is not authorized.

(c) Tell the requester if a record exists and how to review the record. If possible, respond to requests within 10 workdays of receiving them. If you cannot answer the request in 10 workdays, send a letter explaining why and give an approximate completion date no more than 20 workdays after the first office received the request.

(d) Show or give a copy of the record to the requester within 30 workdays of receiving the request unless the system is exempt and the Air Force lists the exemption in appendix C of this part; or published as a final rule in the FEDERAL REGISTER. Give information in a form the requester can understand.

(e) If the requester wants another person present during the record review, the system manager may ask for

<sup>1</sup>Copies may be obtained at cost from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.